Information security essentials

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 mars 2022

https://www.bortzmeyer.org/info-sec-essentials.html

Auteur(s) : Susan McGregor
ISBN n°9-780231-192330
Éditeur : Columbia University Press
Publié en 2021

Un livre très utile <https://cup.columbia.edu/book/information-security-essentials/9780231192330> pour les personnes non expertes en cybersécurité mais qui veulent se protéger un peu plus. L'auteure vise essentiellement les journalistes (le sous-titre est « *"A guide for reporters, editors and newsroom leaders"* ») mais une bonne partie du livre s'applique à tous ceux et à toutes celles qui courent des risques dans le monde numérique (c'est-à-dire à peu près à tout le monde).

Je préviens mes lecteurs et lectrices qui travaillent dans la cybersécurité : ce livre <https://cup.columbia.edu/book/information-security-essentials/9780231192330> n'est pas prévu pour vous. Il ne s'agit pas de devenir expert·e en sécurité informatique, mais d'améliorer sa protection. Et l'auteure ne parle pas que de technique, vous ne trouverez pas de comparaison détaillée de la sécurité de RSA et d'ECDSA, ce n'est pas le sujet.

Susan McGregor part de nombreux cas concrets de problèmes rencontrés par des journalistes, de la confiscation de l'ordiphone par la police pendant une manifestation de Black Lives Matter aux risques de fouille de l'ordinateur qu'on a laissé dans sa chambre pendant un reportage dans un pays peu regardant sur les droits humains. Les risques informatiques sont très nombreux, et certains ne menacent pas que le ou la journaliste mais aussi ses contacts. Et il y a également le risque d'être victime de faux, et de contribuer involontairement à diffuser des mensonges.

McGregor cite de nombreux professionnels des médias, ainsi que des responsables de la sécurité informatique dans divers médias (comme Runa Sandvik). La première partie du livre est une très bonne explication, très pédagogique, du monde numérique. Elle parle ensuite de la délicate mais indispensable modélisation de la menace (oui, vous pouvez être menacé·e, même si vous ne faites pas un reportage sur les djihadistes ou sur les proxénètes). Cette modélisation dépend, l'auteure insiste sur ce point, de la personne concernée : couvrir une manifestation contre les violences policières n'entraine pas les mêmes risques si le journaliste est noir ou blanc.

L'auteure continue avec des conseils pratiques. Pas les ridicules « n'ouvrez pas les pièces jointes provenant d'inconnus » (il serait pratique, le travail journalistique, si ce conseil était suivi) mais plutôt des conseils concrets et réalistes, qui peuvent faire une différence tout de suite (séparez vos comptes personnels et professionnels sur les réseaux sociaux, utilisez un gestionnaire de mots de passe, sauvegardez <https://framablog.org/2021/04/23/sauvegardez/>, chiffrez tout, utilisez l'authentification à deux facteurs, etc). Et elle explique bien qu'aucune solution technique n'est parfaite, il n'y a pas de sécurité absolue, il faut juste pouvoir être capable de déterminer si une solution de sécurité en vaut la peine ou pas.

Le livre détaille la question du reportage à l'étranger, en suggérant de ne pas laisser grand'chose sur son ordinateur, de tout mettre chez des prestataires externes. Cela suppose que ceux-ci soient de confiance. Bien qu'elle soit bien consciente que les États-Unis ne soient pas un pays parfait pour le respect des droits des journalistes, elle ne rappelle hélas pas les risques associés à ces prestataires. Mais il est clair qu'il n'y a pas de solution parfaite. Si on est en reportage en Chine, les fichiers qui restent sur le PC portable sont à la merci de la police chinoise, si on envoie tout chez les GAFA, les fichiers sont à la merci des services étatsuniens. Tout dépend de qui est le plus menaçant, pour un reportage donné.

Ensuite, McGregor étudie comment développer une culture de sécurité, c'est-à-dire comment faire que les bons conseils soient réellement appliqués. Elle est bien consciente que la sécurité, c'est pénible, et que bien des personnes en danger vont prendre des risques alors qu'elles sont informées de ces risques. Le livre couvre donc aussi ces questions plus psychologiques qu'informatiques.

Un chapitre est consacré aux "*freelances*", une catégorie fréquente dans les médias, et qui posent des problèmes de sécurité particulièrement aigus puisqu'ielles ne bénéficient pas forcément des outils de l'organisation qui les emploie, et qu'ielles sont prêt·es à prendre beaucoup de risques déraisonnables, par exemple pour décrocher un "*scoop*". L'auteure insiste donc sur la responsabilité du média, qui ne doit surtout pas encourager cette prise de risques.

Je ne suis pas d'accord avec tout (l'encadré sur logiciel libre vs. privateur est très contestable) mais c'est un livre que je recommande fortement si vous êtes journaliste, ou si vous exercez un autre métier incluant un risque informatique.

(Et, sinon, vous avez un interview de l'auteure en français <https://www.lemonde.fr/blog/binaire/2014/11/05/susan-mcgregor-journaliste-et-informaticienne/>, datant d'avant la parution de son livre.)